FEDERAL BUREAU OF INVESTIGATION
FOI/PA
DELETED PAGE INFORMATION SHEET
FOI/PA# 1329705-0

Total Deleted Page(s) = 22
Page 4 ~ b7E;
Page 14 ~ b7E;
Page 15 ~ b7E;
Page 16 ~ b7E;
Page 17 ~ b7E;
Page 18 ~ b7E;
Page 19 ~ b7E;
Page 20 ~ b7E;
Page 21 ~ b7E;
Page 22 ~ b7E;
Page 23 ~ b7E;
Page 24 ~ b7E;
Page 25 ~ b7E;
Page 26 ~ b7E;
Page 27 ~ b7E;
Page 28 ~ b7E;
Page 29 ~ b7E;
Page 44 ~ b6; b7C; b7D; b7E;
Page 46 ~ Duplicate;
Page 47 ~ Duplicate;
Page 48 ~ Duplicate;
Page 50 ~ b7E;

XXXXXXXXXXXXXXXXXXXXXXXX
X Deleted Page(s) X
X No Duplication Fee X
X For this Page X
XXXXXXXXXXXXXXXXXXXXXXXX

FD-801 (Rev. 7-15-97)

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE **Date:** 11/17/2000

To: Counterterrorism **Attn:** [redacted] b7E

From: SAC, Seattle
Squad 11, IOS [redacted] (206) 262-2438 b6 b7C

Approved By: [redacted]

Drafted By: [redacted] :ljs

Case ID #: ✓288A-SE-~~NEW~~85166-1

Title: Subject: HACKWEISER;
Victim: SNONET;
Type: INTRUSION - WEB PAGE DEFACEMENT;
Date: 09/24/00

SUBMISSION: X Initial ☐ Supplemental ☐ Closed

CASE OPENED: 11/17/00

CASE CLOSED:

☐ No action due to state/local prosecution (Name/Number_____)
☐ USA declination
☐ Referred to Another Federal Agency (Name/Number:_____)
☐ Placed in unaddressed work
☐ Closed administratively
☐ Conviction

COORDINATION: FBI Field Office FBI-[redacted] SA [redacted] b6 b7C b7D
Government Agency _____
Private Corporation _____

VICTIM

Company name/Government agency: SNONET, Contact [redacted]
Address/location: 917 134th Street SW, Suite B-3, Everett, WA b6 b7C b7E
[redacted]
[redacted]

b7E

REMARKS

On September 25, 2000, [redacted] date of birth [redacted] 917 134th Street Southwest, Suite B-3, Everett, Washington, telephone number [redacted] contacted the complaint desk at the Federal Bureau of Investigation (FBI) Seattle, Washington, and advised that his business' web site had been hacked. [redacted] said that the hacker(s) replaced web pages with inappropriate material (e.g., vulgar comments). On November 17, 2000, Intelligence Operations Specialist (IOS) [redacted] telephonically contacted [redacted] who provided the following information:

b6
b7C

[redacted] is the Manager of Technical Services for SnoNet, a company that provides web hosting for Western Washington non-profit organizations. In September 2000, four web sites hosted by SnoNet were defaced: the SnoNet.org site, the Cleveland High School Alumni Association site, Snohomish County Tourism's "Grandparents Stay Free" site, and the Washington Red Cross' site. The hacker(s) replaced material on the SnoNet hosted web sites with profane messages. [redacted] does not know the true identity of the hackers. [redacted] could not recall the names or Pseudemys the hacker(s) used, but advised that mirrored pages were posted on Attrition's web site (www.attrition.org).

b6
b7C

[redacted] said the SnoNet web host runs Windows NT 4.0 as its operating system. [redacted] said that the hacker(s) broke into the SnoNet web host via vulnerability found in "mdac" [redacted] consequently patched the mdac vulnerability.

b6
b7C
b7E

SnoNet does not utilize anti-virus software or firewalls on its web hosts. [redacted] said he updates access control lists and runs a DMZ (Demilitarized Zone) host as a security

b6
b7C

precaution. Warning banners are not posted by SnoNet on their hosted sites. [redacted] said he doesn't know why someone would want to hack into a non-profit site, a medium that is in place only to help people. [redacted] said he would provide the FBI logs documenting the intrusion. b6 b7C

On November 17, 2000, and November 20, 2000, IOS [redacted] b6 b7C b7E

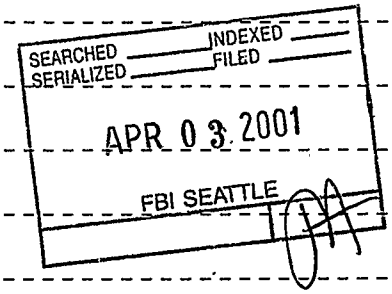
[redacted] b7E

322ljs01.801

1A Envelope

Case ID: 288A-SE-85166

SE 1	ORIGINAL NOTES RE INTERVIEW OF: [redacted] ON 11/17/00	b6 b7C



FD-340a (Rev. 11-12-89)

(Title) _____

(File No.) _____

Item	Date Filed	To be returned			Disposition
		Yes	No		

FD-340 (Rev. 8-7-97)

85160-1A1

Universal Case File Number 288A-SE-[illegible]

Field Office Acquiring Evidence SE

Serial # of Originating Document

Date Received 11/17/00

From IOS [redacted] b6 b7C
(Name of Contributor)

1110 Third Ave.
(Address of Contributor)

Seattle, WA 98101
(City and State)

By IOS [redacted]
(Name of Special Agent)

To Be Returned ☐ Yes ☑ No
Receipt Given ☐ Yes ☑ No
Grand Jury Material - Disseminate Only Pursuant to Rule 6 (e)
Federal Rules of Criminal Procedure
☐ Yes ☑ No

Title:

Reference:
(Communication Enclosing Material)

Description: ☑ Original notes re interview of

11/17/00 Interview of [redacted] b6 b7C

KEEP ATTACHED TO
SEATTLE EXHIBIT
288A-SE-85166-1A|

11/17/00:

SNONET is a Technology company that does web hosting for non-profits WEstern Washington.

[redacted] snonet, recross@washington, clearwater school, and (no contact with the subject)..cleavand higschool alum,ni assoc, snohomish country tourism grandparentsstayfree.com site. b7E

WinNT 4.0 IIS service.
mdac sql statements, the mdac component, the webserver interacts, he did somehtings via sql.
patched.

no ant-virus, does not have a real firewall but uses some access lists and a dmz host).

BIg hassle, should have updated any way, three hours to repair the damage.

some banner warnings on the intranet not on the internet.

[redacted] is the Magager of technical services. b6 b7C

no identified logging information where the person connected from: but will send me his logs.

doesn't know who did the hack.

his freq. scanned.

KEEP ATTACHED TO
SEATTLE EXHIBIT
288A -SE- 85166 -1A|

25
Sept 2000

FD-71 (Rev. 3-27-95)
Complaint Form

NOTE: Hand print names legibly; handwriting satisfactory for remainder.
Indices: ☐ Negative ☐ See below

Subject's name and aliases	Character of case
UNSUB;	Computer Intrusion;
	Complainant ☐ Protect Source [redacted] b6 b7C
	Complaint received ☐ Personal ☒ Telephonic Date 09/25/2000 Time 11:35 am
Address of Subject	Complainant's address and telephone number 917 134th Street Southwest, Ste B-3 Everett, WA. (425) 921-3471
	Complainant's DOB 11/05/1964 / Sex Male

Subject's Description						
	Race	☐ Male	Height	Hair	Build	Birth date and birth place
	Age	☐ Female	Weight	Eyes	Complexion	Social Security Number
	Scars, marks and other data					

Employer	Address	Telephone

Vehicle Description

Facts of Complaint

C called Seattle FBI to report that the web site for his place of business, "SNONET", a non-profit organization in Everett, Washington had been "hacked" into. C claims that four pages of about sixty have inappropriate material, i.e. vulgar comments, etcetera.

288A-SE-85166-2

aeg
(2)

Do not write in this space.

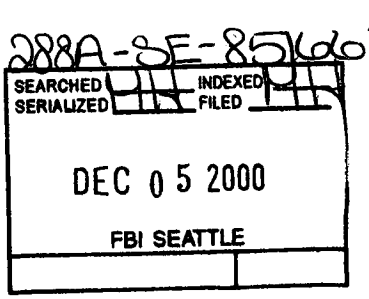
SEARCHED ____ INDEXED ____
SERIALIZED ____ FILED ____
DEC 0 1 2000
FBI SEATTLE

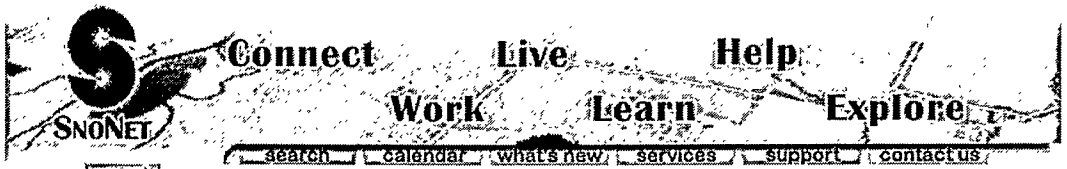
[redacted] b6 b7C
(Complaint received by)

BLOCK STAMP

269-150703-FD71

288A-SE-85460-3





search

Welcome

917 - 134th St. S.W.
Suite B3
Everett, WA 98204-9377

info@snonet.org

Tel: 425.921.3473
Fax: 425.921.3484

SnoNet the Organization

Who We Are

How To Help

Feedback

Newsletter

Services

Projects

Sites Hosted On SnoNet

MEMBER A.F.C.N. Association FOR Community Networking

A Connected Community is about Partnerships. Visit Our Featured Sites and Partners listed below as well as the other sites we host. Also check out Teens4teens the teen issues Web site, MATCHES our system for matching School-to-Work opportunities, and **The Regional Skills Gap Consortium** site.

Featured Sites

Thanks for coming to SnoNet, gateway to Snohomish County, Washington, where business, education, community services and local government are working together to create an interconnected community for the 21st century. If you would like more background info on SnoNet it is available in the organization section of the site, or read about the many services we provide to the

Events

Closing ceremony of YMCA Connections, a week-long retreat at Warm Beach that brings together teens & cops to discuss DUI, drug use, and violence, and create action plans for their community. Ceremony begins at 10:30am and ends at noon on 11/10/2000. Closing speaker is Lieutenant Governor Brad Owen.

--

community. This is a community resource and will improve and meet the needs of the community if you add your voice.

[Explore] [Work] [Live] [Learn] [Help] [Connect]
[search] [calendar] [what's new] [contact us] [services] [support]

Please check out our sponsors!

Please send us your links, events, or comments.

SnoNet - Who or what are we?

Who We Are

SnoNet the Organization

Who We Are

- Sponsors
- Contact Us
- Mission/History

How To Help

Feedback

Newsletter

Services

Projects

SnoNet is based on a strong community partnership. SnoNet has a 120 person steering committee that helped develop the original vision for SnoNet. The steering committee now meets annually to review the progress of SnoNet. SnoNet has a 9 member board of directors that represent key partners in the region. The ten members of the SnoNet staff team serve to direct the projects of SnoNet and implement the workplan.

U.S. Secretary of Education Richard Riley & U.S. Senator Patty Murray get a briefing on SnoNet & SchoolWork by SnoNet & SchoolWork Initiative Board members.

Board of Directors

- **Burnie Clark**, President/CEO, KCTS-TV
- **Jack Corbally**, Chairman, The MacArthur Foundation
- **Bob Drewel**, County Executive, Snohomish County
- **Charlie Earl**, President, Everett Community College
- **Larry Hanson**, President and Publisher, The Herald
- **Charlie Liekweg**, President/CEO, AAA of Washington
- **Dr. Wayne Robertson**, Superintendent, Edmonds School District
- **Brent Stewart**, President, United Way of Snohomish County
- **John Thoresen**, President, Mutual Bancshares Capital

Sponsored in part by:

Please send us your links, events, or comments.

Server Insecurity

By Saumil Udayan Shah
(6/13/00)

Microsoft IIS MDAC RDS Vulnerability

Servers affected: Windows NT servers running IIS 4.0 with MDAC version 2.1 or earlier

About a month after the IIS eEye hack was discovered, another vulnerability in IIS 4.0 popped up. Using Microsoft Data Access Components (MDAC) and Remote Data Services (RDS), an attacker can establish unauthorized ODBC connections and gain access to internal files on the Web server. If either the Microsoft Jet OLE DB provider or the datashape provider is installed, an attacker can issue commands to be executed on the server using the Visual Basic for Applications shell() function.

The MDAC RDS vulnerability can be found in IIS 4.0 with MDAC version 2.1 or lower, in the \msadc\msadcs.dll file in the Web server public directory. Rain Forest Puppy includes the details of this hack on his site. The exploit makes use of improper configuration and lack of security mechanisms from the default installation of MDAC on IIS. In this attack, someone can remotely execute arbitrary commands on the NT system under the security privilege context of the IIS Web server process, which is equivalent to the NT Administrator.

MDAC's vulnerability lies not in the technology but rather in the way users configure it. Many sites install IIS 4.0 from NT Option Pack 4.0. If the NT Option Pack 4.0 is installed with the Typical or default configuration settings, MDAC is vulnerable to this attack. Most system administrators using the default setup had not hardened the Web server security by fine-tuning the settings.

George Kurtz of Foundstone Inc., Nitesh Dhanjani of Purdue University, and I devised a one-line command string to be used with the MDAC RDS exploit that caused the remote NT system to initiate a file transfer over FTP or TFTP. Our command tells the server to download and execute Netcat from an outside system. Netcat will run the Windows command shell and establish a connection back to the attacker's computer, giving the attacker full administrative control of the remote NT system.

Microsoft has posted a security bulletin describing the procedure to secure IIS 4.0 against this vulnerability.

Break in through ColdFusion

Microsoft IIS ism.dll Buffer Overflow
Microsoft IIS MDAC RDS Vulnerability
Allaire ColdFusion 4.0 Vulnerabilities
Sambar 4.3 hello.bat

Saumil Udayan Shah, principal consultant for Foundstone Inc., provides information security consulting services to Foundstone clients. Shah specializes in ethical hacking and security architecture. He holds a designation as a Certified

Information Systems Security Professional (CISSP).

Microsoft Security Program: Frequently Asked Questions: Microsoft Security Bulletin (MS99-025)

What's this bulletin about?

Microsoft Security Bulletin MS99-025 is a re-release of Microsoft Security Bulletin MS98-004, which was originally issued on July 17, 1998, and discussed a vulnerability in the Microsoft® Data Access Components (MDAC). A visitor to a web site on which both Microsoft Internet Information Server (IIS) and certain versions of MDAC are installed could perform privileged actions on the system. IIS and MDAC 1.5 are installed by default as part of the Windows NT 4 Option Pack.

Microsoft takes security seriously, and is providing this bulletin to remind customers about this vulnerability, to restate the threat, and encourage system administrators to evaluate their systems to determine if their systems have been correctly configured and updated to protect against this vulnerability.

What's the scope of the vulnerability?

This is a privilege elevation attack. On a system with both IIS and MDAC installed, the vulnerability in MDAC could allow an otherwise unauthorized web user to perform privileged actions on the system, including:

- Allowing an unauthorized user to execute shell commands on the IIS system as a privileged user.
- On a multi-homed Internet-connected IIS system, using MDAC to tunnel SQL and other ODBC data requests through the public connection to a private back-end network.
- Allowing unauthorized access to secured, non-published files on the IIS system.

Is this a new issue?

No. It was previously discussed in Microsoft Security Bulletin MS98-004, which documented the vulnerability in MDAC 1.5 and detailed steps that should be taken to eliminate the vulnerability. Customers who followed steps detailed in MS98-004 are not at risk from this vulnerability.

If this is not a new issue, why is Microsoft re-releasing the security bulletin?

There are three reasons:

- Microsoft has recently learned that the vulnerability has been used to gain unauthorized access to Internet-connected systems that have not been updated per the instructions in MS98-004.
- Unlike many vulnerabilities, this one is not eliminated simply by upgrading to a subsequent version. When upgrading, customers need to either perform a clean install or set a particular registry key to ensure that they are not vulnerable to the problem.

- If a set of sample pages has been installed on a production server, it can introduce the vulnerability into an otherwise-secured server.

The intent of re-releasing this bulletin is to serve as a reminder about this vulnerability, to restate the threat, and encourage system administrators to evaluate their systems to determine if their systems have been correctly configured and updated to protect against this vulnerability.

I have a firewall that protects my web server, will it protect me from this vulnerability?

In most cases, a simple packet-filtering firewall will not prevent exposure to this vulnerability. The RDS DataFactory object can be invoked by a web client issuing standard URL requests to an Internet Information Server over port 80 (or any alternate port that you have configured IIS to listen to).

Is this a vulnerability in IIS?

No. The only reason that IIS is discussed with regard to this vulnerability is because IIS provides a means for a hostile user to remotely exploit the vulnerability.

Where does the vulnerability lie?

The vulnerability lies in the Microsoft Data Access Components (MDAC); specifically, in one component of the Remote Data Services in MDAC, the DataFactory object.

MDAC provides key technologies that enable Universal Data Access. Data-driven client/server applications deployed over the Web or a LAN can use these components to easily integrate information from a variety of sources, both relational (SQL) and nonrelational. These components include Microsoft ActiveX® Data Objects (ADO), OLE DB, and Open Database Connectivity (ODBC). MDAC 1.5 ships with the Windows NT 4.0 Option Pack, and is installed during a default installation of the Option Pack.

Remote Data Service (RDS) is a component of MDAC which is installed by default when installing the Microsoft Windows NT 4.0 Option Pack. The goal of the RDS component is to enable controlled Internet access to remote data resources through IIS. A component of RDS, called the DataFactory object, is where the vulnerability is. The DataFactory object is designed as a server-side Automation object that receives client requests. In an Internet implementation, it resides on a Web server and is instantiated by the ADISAPI component. The DataFactory object provides read and write access to specified data sources, but doesn't contain any validation or business rules logic.

What versions of MDAC are affected?

- MDAC 1.5 and 2.0 are affected by the vulnerability.
- MDAC 2.1 is affected by the vulnerability when installed as an upgrade from a previous version.
- Clean installations of MDAC 2.1 are only affected if Sample Pages for RDS have been installed.

What are Sample Pages for RDS?

These are samples provided as part of the Windows NT 4.0 Option Pack and the MDAC 2.0 Software Developers Kit (SDK). They are intended to help customers learn how to use the Remote Data Services, but are not intended to

be deployed on production servers. The samples are not installed by default in the Option Pack, but are installed by default in the MDAC 2.0 SDK.

What do I need to do?

You need to do three things:

1. Determine what version of MDAC you are running, then consult the instructions below to configure it for secure operation.
2. Determine whether you need RDS functionality, then consult the instructions below to either disable it or configure it for secure operation. If you don't need it, the safest course of action is to disable it.
3. Determine whether you installed the Sample Pages for RDS. If you did, you should remove them.

How do I determine what version of MDAC I have installed?

You can check the version numbers on specific .dll files associated with MDAC to determine the version installed on your system. The following table summarizes what file versions correspond to which MDAC versions.

MDAC version	Msdadc.dll	Oledb32.dll	Notes
MDAC 1.5c	1.50.3506.0	N/A	
MDAC 2.0	2.0.3002.4	2.0.1706.0	
MDAC 2.0 SP1	2.0.3002.23	2.0.1706.0	
MDAC 2.0 SP2	2.0.3002.23	2.0.1706.0	Superset: SP1
MDAC 2.1.0.3513.2 (SQL)	2.10.3513.0	2.10.3513.0	
MDAC 2.1.1.3711.6 (Internet Explorer 5)	2.10.3711.2	2.10.3711.2	
MDAC 2.1.1.3711.11 (GA)	2.10.3711.2	2.10.3711.9	

Note these version numbers and compare them after an application installation to determine whether MDAC was upgraded. We also encourage you to view the MDAC Release Manifest for more information about MDAC versioning.

I have MDAC 1.5 installed. What should I do?

If you need RDS functionality, you'll need to install MDAC 2.1, then follow the instructions below for securing your MDAC 2.1 installation. If you don't need RDS functionality, you should remove it by following the instructions below under "*I don't need the RDS functionality. How do I remove it?*".

I have MDAC 2.0 installed. What should I do?

You need to configure MDAC to operate in "safe mode". This provides RDS functionality but eliminates the vulnerability. "Safe mode" is governed by the setting of the following registry value:

Hive	HKEY_LOCAL_MACHINE \SOFTWARE
Key	Microsoft\DataFactory\HandlerInfo\
Name	HandlerRequired
Type	DWORD
Value	0="unsafe mode" 1="safe mode"

To make it easier to ensure that the server is configured in "safe mode", we provide a .REG file that when run on a system will set the appropriate registry key automatically. To use this .REG file, do the following:

- The file is packaged as a self-extracting .zip file. Click here, then choose to either save or run the self-extracting file.
- Run the self-extracting .zip file to extract the file it contains, which is named HANDSAFE.REM.
- When you are ready to make the registry changes, rename HANDSAFE.REM to HANDSAFE.REG. (We packaged the file with an .REM extension as a safety measure -- .REG files automatically launch when double-clicked.)
- Copy HANDSAFE.REG to each system that requires the registry change. Double Click HANDSAFE.REG to make the change.

I installed MDAC 2.1 as an upgrade. What should I do?

You need to configure MDAC to operate in "Safe Mode". See "*I have MDAC 2.0 installed. What should I do?*" for instructions.

I installed MDAC 2.1 as a clean installation. What should I do?

Clean installations of MDAC 2.1 are already configured in "safe mode".

I have MDAC 2.1 installed, but I don't know whether I did a clean install or an upgrade. What should I do?

As long MDAC 2.1 is configured for "safe mode", it doesn't matter how it was installed. The important point is that clean installations of MDAC 2.1 default to "safe mode", and upgrades default to "unsafe mode". If you're not sure how you installed MDAC 2.1, it won't hurt to run HANDSAFE.REG, or to make the registry changes manually.

I don't need RDS functionality. What should I do?

Regardless of the version of MDAC you're using, you can disable RDS functionality by doing the following:

1. Delete the /msadc virtual directory from the default Web site

Remove the following registry keys from the server hosting IIS:

- HKEY_LOCAL_MACHINE \SYSTEM \CurrentControlSet \Services \W3SVC \Parameters \ADCLaunch \RDSServer.DataFactory
- HKEY_LOCAL_MACHINE \SYSTEM \CurrentControlSet \Services \W3SVC \Parameters \ADCLaunch \AdvancedDataFactory
- HKEY_LOCAL_MACHINE \SYSTEM \CurrentControlSet \Services \W3SVC \Parameters \ADCLaunch \VbBusObj.VbBusObjCls

Actually, performing either of the above steps will disable RDS functionality. However, we've listed both steps for completeness.

I do need RDS functionality. What should I do?

The DataFactory object provides powerful capabilities that web developers can use to build applications which access a rich variety of data sources. Best practices for applications that use RDS functionality include:

- Ensure that you have installed the latest version of MDAC on your system, and configured it to run in "safe mode".
- Ensure that the Sample Pages for RDS are not installed.
- If anonymous users should not be able to use RDS, disable Anonymous Access for the /msadc directory in the default Web site.
- If you want to only allow specific database requests, you can create a custom handler to control or filter incoming requests. Information on how to do this is available at http://www.microsoft.com/Data/ado/rds/custhand.htm

I installed the Sample Pages for RDS. What should I do?

The sample pages are not intended for use on production servers. In particular, the VbBusObj object, which is installed as part of the sample pages, provides an additional means of exploiting the same vulnerability. At minimum, you should ensure that the VbBusObj object is removed by doing the following:

- Delete %systemdrive%\program files\common files\system\msadc\samples\selector\middle_tier\vbbusobj\vbbusobj.dll
- Remove the registry key HKEY_LOCAL_MACHINE/System/CurrentControlSet/Services/W3SVC/Parameters/ADCLaunch/VbBusObj.VbBusObjCls

However, the best practice is to remove the samples altogether. To do this, delete the contents of %systemdrive%\program files\common files\system\msadc\samples and all subfolders.

I don't know whether I installed the sample pages or not. What should I do?

If the folder %systemdrive%\program files\common files\system\msadc\samples exists, the sample files are installed, and you should remove that folder and all subfolders.

I installed the default installation of the Windows NT 4.0 Option Pack, am I affected?

Yes. The default installation of the Windows NT 4.0 Option Pack installs Microsoft Internet Information Server 4.0 and Microsoft Data Access

Components 1.5, which is a vulnerable configuration.

Can I install the Windows NT 4.0 Option Pack without installing MDAC 1.5?

Yes. You can perform a custom installation of the Windows NT 4.0 Option Pack, and specify that the MDAC components should not be installed.

I installed the Windows NT 4.0 Option Pack, and then installed Windows NT 4.0 Service Pack 4 or 5, am I still affected?

Unless you have taken the steps indicated above (and in MS98-004), your system is still vulnerable. Service Packs 4 and 5 do not automatically update the MDAC components, nor do they automatically disable the DataFactory object.

Is there something I can watch for in the logs to help determine if someone is trying to use this vulnerabilty to gain access to my system?

Since exploiting this vulnerability requires a standard HTTP "POST" to the MDAC DataFactory object, you might be able to detect that someone has attempted to use this vulnerability against your system by reviewing the IIS logs for "POST" entries to /msadc/msadcs.dll.

Since the DataFactory object is a standard programmable interface, POST requests could be generated as part of the normal functioning of a custom-built web application. However, IIS does not use this functionality by default. So, unless you have built a custom application that uses the DataFactory object, a "POST /msadc/msadcs.dll" log entry indicates a good chance that someone has attempted to use this vulnerability against your system.

However, it is important to realize that if someone has gained privileged access to your system by exploiting this vulnerability, it may be possible for them to alter the IIS data logs.

I have some questions about installing MDAC 2.0 or 2.1, where can I find more information?

Information about the Microsoft Data Access Components can be found on the Microsoft Universal Data Access web site at http://www.microsoft.com/data. Questions specific to installing MDAC can be found on the MDAC Installation FAQ, http://www.microsoft.com/data/MDAC21info/MDACinstQ.htm.

Where can I get the latest version of MDAC?

You can download the latest versions of MDAC from the Microsoft Universal Data Access download site, http://www.microsoft.com/data/download.htm

Where can I learn more about securing an Internet-based IIS server?

A good resource for securing a system running Internet Information Server 4.0 is the Microsoft Internet Information Server 4.0 Security Checklist, http://www.microsoft.com/technet/security/iischk.asp.

Where can I learn more about best practices for my network?

The Microsoft Security web site is the best to place to get information about Microsoft security.

How do I get technical support on this issue?

Microsoft Data Access Components (MDAC) is a fully supported set of technologies. If you require technical assistance with this issue, please contact Microsoft Technical Support. Information on contacting Microsoft Technical Support is available at http://support.microsoft.com/support/contact/default.asp.

THE INFORMATION PROVIDED IN THE MICROSOFT KNOWLEDGE BASE IS PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND. MICROSOFT DISCLAIMS ALL WARRANTIES, EITHER EXPRESS OR IMPLIED, INCLUDING THE WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. IN NO EVENT SHALL MICROSOFT CORPORATION OR ITS SUPPLIERS BE LIABLE FOR ANY DAMAGES WHATSOEVER INCLUDING DIRECT, INDIRECT, INCIDENTAL, CONSEQUENTIAL, LOSS OF BUSINESS PROFITS OR SPECIAL DAMAGES, EVEN IF MICROSOFT CORPORATION OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. SOME STATES DO NOT ALLOW THE EXCLUSION OR LIMITATION OF LIABILITY FOR CONSEQUENTIAL OR INCIDENTAL DAMAGES SO THE FOREGOING LIMITATION MAY NOT APPLY.

Last updated January 4, 2000

CNET

CNET glossary

ODBC

Open Database Connectivity

This set of application programming interfaces, created by Microsoft, defines how to move information in and out of any PC database that supports the standard.

See also: API

FD-801 (Rev. 7-15-97)

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE **Date:** 08/08/2001

To: Counterterrorism **Attn:** [redacted] b7E
[redacted] Room 5965
[redacted]

From: SAC, Seattle
Squad 11
Contact:

Approved By: [redacted] b6 b7C

Drafted By: [redacted] dgt

Case ID #: 288A-SE-85166

Title: Subject: HACKWEISER;
Victim: SNONET;
Type: Intrusion - Web Page Defacement
Date: 09/24/2000

SUBMISSION: ☐ Initial ☐ Supplemental ☒ Closed

CASE OPENED: 11/17/2000

CASE CLOSED: 08/08/2001

☐ No action due to state/local prosecution (Name/Number_____)
☒ USA declination
☐ Referred to Another Federal Agency (Name/Number:_____)
☐ Placed in unaddressed work
☐ Closed administratively
☐ Conviction

COORDINATION: FBI Field Office Settle
Government Agency N/A
Private Corporation SNONET contact [redacted] b6 b7C
VICTIM

[redacted] b7E

[redacted]

288A-SE-85166-9
FAH MAH
2001

b7E

REMARKS

On 09/25/2000, [redacted] contacted the complaint desk of the Seattle Division of the Federal Bureau of Investigation. [redacted] advised that his business' web site had been hacked, and that hacker(s) had replaced web pages with inappropriate material (e.g. vulgar comments). On 11/17/2000, Intelligence Operations Specialist (IOS) [redacted] telephonically contacted [redacted] For a full accounting of [redacted] statement, please see the 801 in this case dated 11/17/2000. A case, predicated on a violation of 18 U.S.C. 1030, was opened. The case was assigned to writer on 12/01/2000.

b6
b7C

[redacted]

b7D
b7E

On 08/08/2001 during a meeting with the United States Attorney's Office, AUSA [redacted] declined prosecution of the above caption case. As a result, the Seattle Division of the FBI is closing its file.

b6
b7C
b7E

[redacted]